

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 10320357 A

(43) Date of publication of application: 04 . 12 . 98

(51) Int. Cl.

G06F 15/00  
G06F 1/00

(21) Application number: 09127291

(22) Date of filing: 16 . 05 . 97

(71) Applicant: PFU LTD

(72) Inventor: MIMURA MASAHIRO  
MAEDA KIYOTAKA

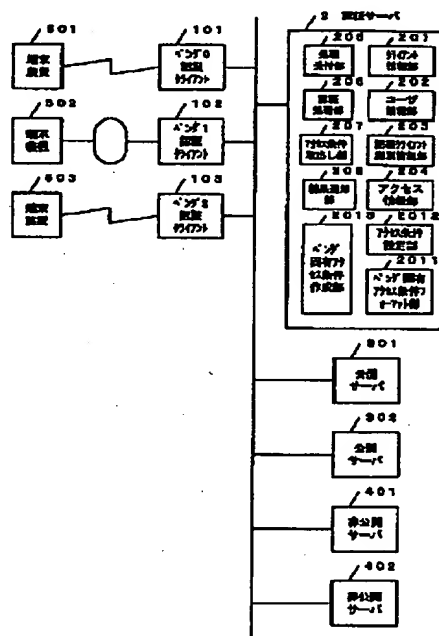
(54) CERTIFICATION SERVER IN USER  
CERTIFICATION SYSTEM, METHOD FOR  
CERTIFYING THE SAME AND RECORDING  
MEDIUM FOR THE METHOD

(57) Abstract:

PROBLEM TO BE SOLVED: To attain the unitary management of user certification by accepting certification requests issued from plural different bender certification clients by only one certification server.

SOLUTION: In this certification server 2, a certification client identification information part 203 stores a bender ID, edition number, group, and level or the like. An access information part 204 stores an access class, bender ID, edition number, group, and access condition or the like. An access condition extracting part 207 extracts an access condition corresponding to a certification request from an access information part. Thus, the unitary management of user certification can be attained by only one certification server.

COPYRIGHT: (C)1998,JPO





(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-320357

(43) 公開日 平成10年(1998)12月4日

(51) Int.Cl. <sup>8</sup>	識別記号	F I	
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B
1/00	3 7 0	1/00	3 7 0 E

審査請求 未請求 請求項の数 6 O L (全 12 頁)

(21) 出願番号 特願平9-127291

(22) 出願日 平成9年(1997)5月16日

(71) 出願人 000136136

株式会社ピーエフユー

石川県河北郡宇ノ気町宇野気ヌ98番地の  
2

(72) 発明者 三村 昌裕

石川県河北郡宇ノ気町宇野気ヌ98番地の  
2 株式会社ピーエフユー内

(72) 発明者 前田 清隆

石川県河北郡宇ノ気町宇野気ヌ98番地の  
2 株式会社ピーエフユー内

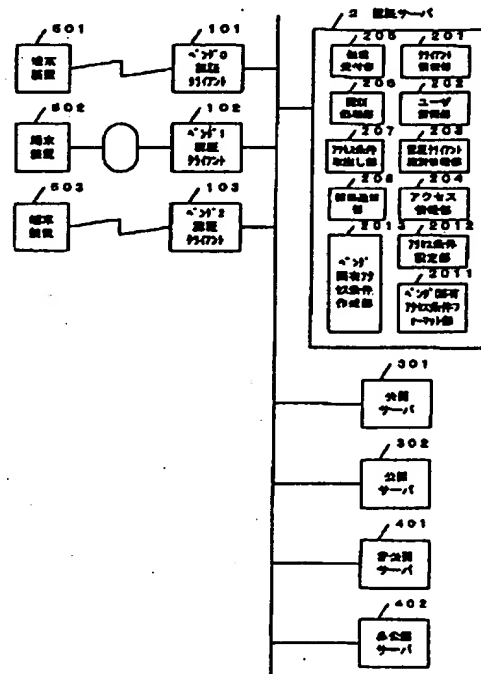
(54) 【発明の名称】 ユーザ認証システムにおける認証サーバおよびその認証方法およびその記録媒体

(57) 【要約】

【課題】 ユーザ認証システムにおいて、異なるベンダの認証クライアントが混在する場合、各ベンダの認証クライアントの仕様が細かい所で違い、通知される認証情報に互換性がなく、また、他のベンダと差別化を図るため、標準規格のアクセス条件の他に固有のアクセス条件の設定を設けている。このため、認証サーバは、ベンダ毎に用意する必要があり、また、固有のアクセス条件を使用する場合は、ベンダ毎にアクセス条件を定義する必要があるという問題点があった。

【解決手段】 ベンダID、版数、グループ、レベルなどを記憶する認証クライアント識別情報部と、アクセスクラス、ベンダID、版数、グループ、アクセス条件などを記憶するアクセス情報部と、認証要求に対応するアクセス条件をアクセス情報部から取出すアクセス条件取出し部とを認証サーバに設けることにより、認証サーバを一つにし、ユーザ認証の一元管理を行う。

本発明のユーザ認証システムの構成ブロック例図



## 【特許請求の範囲】

【請求項1】 認証クライアントのIPアドレス、レベル、認証キーなどを記憶するクライアント情報部(201)と、ユーザID、パスワード、アクセスクラスなどを記憶するユーザ情報部(202)と、ベンダID、版数、グループ、レベルなどを記憶する認証クライアント識別情報部(203)と、アクセスクラス、ベンダID、版数、グループ、アクセス条件などを記憶するアクセス情報部(204)と、認証クライアントからの認証要求を受付ける処理受付部(205)と、処理受付部(205)で受付けた認証クライアントのIPアドレスや認証キーおよびユーザIDやそのパスワードなどが接続を許可してよいものかを確認する認証処理部(206)と、処理受付部(205)で受付けた認証クライアントに対応するアクセス条件をアクセス情報部(204)から取出すアクセス条件取出し部(207)と、認証結果およびアクセス条件を認証要求元に通知する結果通知部(208)と、で構成されることを特徴とするユーザ認証システムにおける認証サーバ。

【請求項2】 複数のベンダ固有のアクセス条件フォーマットを記憶するベンダ固有アクセス条件フォーマット部(2011)と、入力されたアクセス条件を記憶部などに格納するアクセス条件設定部(2012)と、ベンダ固有アクセス条件フォーマット部(2011)を参照し、アクセス条件設定部(2012)で格納されたアクセス条件をベンダ固有アクセス条件に変換するベンダ固有アクセス条件作成部(2013)とを備えることを特徴とする請求項1記載のユーザ認証システムにおける認証サーバ。

【請求項3】 ユーザ情報およびクライアント情報の受信手順と、認証クライアントを識別する情報を求める手順と、ユーザに対応するアクセスクラスを求める手順と、認証クライアント識別情報とアクセスクラスからアクセス条件を求める手順とを持つことを特徴とする認証方法。

【請求項4】 アクセス条件の入力手順と、ベンダ固有のアクセス情報フォーマット定義部を読み込む手順と、入力したアクセス条件をベンダ固有のアクセス情報フォーマットに従って定義し直し、ベンダ固有アクセス条件を作成する手順とを持つことを特徴とする認証方法。

【請求項5】 コンピュータに、ユーザ情報およびクライアント情報の受信手順と、認証クライアントを識別する情報を求める手順と、ユーザに対応するアクセスクラスを求める手順と、認証クライアント識別情報とアクセスクラスからアクセス条件を求める手順とを実行させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項6】 コンピュータに、アクセス条件の入力手順と、ベンダ固有のアクセス情報フォーマット定義部を読み込む手順と、入力したアクセス条件をベンダ固有の

アクセス情報フォーマットに従って定義し直し、ベンダ固有アクセス条件を作成する手順とを実行させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ユーザ認証システムにおける認証サーバに関するものであり、特に、異なるベンダのルータおよび異なるソフトウェア版数のルータなどの認証クライアントが混在する環境で、ユーザ認証の一元管理をできるようにする。

【0002】

【従来の技術】図7に、従来のユーザ認証システムの構成ブロック例図を示す。図中、711はベンダ0の製品であるベンダ0認証クライアント、721はベンダ0認証クライアント用の認証サーバであるベンダ0認証サーバ、712はベンダ1の製品であるベンダ1認証クライアント、722はベンダ1認証クライアント用の認証サーバであるベンダ1認証サーバ、713はベンダ2の製品であるベンダ2認証クライアント、723はベンダ2認証クライアント用の認証サーバであるベンダ2認証サーバである。

【0003】また、751、752、753は、各認証クライアントにネットワークで接続された端末装置である。

【0004】また、731、732は、ネットワークに接続された全ての認証クライアントおよびユーザからアクセス可能な公開サーバ、741、742は、ネットワークに接続された一部の認証クライアントまたは一部のユーザだけに公開されている非公開サーバである。

【0005】ユーザが公開サーバまたは非公開サーバにアクセスするとき、認証サーバが認証クライアントから通知されたIPアドレス、認証キー、ユーザID、パスワードなどをもとに、サーバ内で定義されているクライアント情報、ユーザ情報、アクセス情報などと比較し、そのアクセスの許可/拒否などの認証情報を認証クライアントに通知している。

【0006】しかし、各ベンダの認証クライアントの仕様は細かい所で違いがあり、通知される認証情報に互換性がない場合がある。この場合、同一の認証処理部では、正常に処理が行えない。また、各ベンダは他のベンダの認証クライアントと差別化を図るため、標準規格のアクセス条件の他にベンダ固有のアクセス条件の設定を設けている。そして、このベンダ固有のアクセス条件を使用した場合、この認証クライアントに対応する認証サーバが必要となる。

【0007】従って、図7のような異なるベンダの認証クライアントを後から随時追加したようなユーザ認証システムでは、ベンダ毎に認証サーバを設置することになる。

【0008】

【発明が解決しようとする課題】図7に示す従来技術では、異なるベンダの認証クライアントが混在する環境で、ユーザ認証を行う認証サーバは、ベンダ毎に用意する必要があった。また、ベンダ固有のアクセス条件を使用する場合は、ベンダ毎にアクセス条件を定義する必要があるという問題点があった。すなわち、異なるベンダの認証クライアントが混在する環境では、ユーザ情報がそれぞれのサーバに分散するため、ユーザ認証の一元管理ができない、また、システムの追加および変更、ユーザの追加および変更などの管理作業が煩雑になるという問題点があった。

【0009】

【課題を解決するための手段】この発明は上記のような問題点を考慮してなされたもので、ユーザ認証システムにおいて、異なるベンダのルータおよび異なるソフトウェア版数のルータなどの認証クライアントが混在する環境で、ベンダID、版数、グループ、レベルなどを記憶する認証クライアント識別情報部と、アクセスクラス、ベンダID、版数、グループ、アクセス条件などを記憶するアクセス情報部と、処理受付部で受付けた認証クライアントに対応するアクセス条件をアクセス情報部から取出すアクセス条件取出し部とを認証サーバに設けることにより、ユーザ認証の一元管理をできるようにする。

【0010】

【発明の実施の形態】ユーザ認証システムにおける認証サーバを、認証クライアントのIPアドレス、レベル、認証キーなどを記憶するクライアント情報部と、ユーザID、パスワード、アクセスクラスなどを記憶するユーザ情報部と、ベンダID、版数、グループ、レベルなどを記憶する認証クライアント識別情報部と、アクセスクラス、ベンダID、版数、グループ、アクセス条件などを記憶するアクセス情報部と、認証クライアントからの認証要求を受付ける処理受付部と、処理受付部で受付けた認証クライアントのIPアドレスや認証キーおよびユーザIDやそのパスワードなどが接続を許可してよいものかを確認する認証処理部と、処理受付部で受付けた認証クライアントに対応するアクセス条件をアクセス情報部から取出すアクセス条件取出し部と、認証結果およびアクセス条件を認証要求元に通知する結果通知部と、で構成することにより、複数の異なるベンダの認証クライアントから発行される認証要求を唯一つの認証サーバで受付けることが可能となる。

【0011】また、上記の認証サーバに、複数のベンダ固有のアクセス条件フォーマットを記憶するベンダ固有アクセス条件フォーマット部と、入力されたアクセス条件を記憶部などに格納するアクセス条件設定部と、ベンダ固有アクセス条件フォーマット部を参照し、アクセス条件設定部で格納されたアクセス条件をベンダ固有アクセス条件に変換するベンダ固有アクセス条件作成部とを

備えることにより、各ベンダの認証クライアントの仕様を熟知しなくても、迅速かつ容易に作成することが可能となる。

【0012】

【実施例】図1に、本発明のユーザ認証システムの構成ブロック例図を示す。図中、101はベンダ0の製品であるベンダ0認証クライアント、102はベンダ1の製品であるベンダ1認証クライアント、103はベンダ2の製品であるベンダ2認証クライアント、2はベンダ0認証クライアント101、ベンダ1認証クライアント102、ベンダ2認証クライアント103からの認証要求を受付け、認証結果をそれぞれに通知する認証サーバである。

【0013】また、501、502、503は、各認証クライアントにネットワークで接続された端末装置である。

【0014】また、301、302は、ネットワークに接続された全ての認証クライアントおよびユーザからアクセス可能な公開サーバ、401、402は、ネットワークに接続された一部の認証クライアントまたは一部のユーザだけに公開されている非公開サーバである。

【0015】また、認証サーバ2は、認証クライアントのIPアドレス、レベル、認証キーなどを記憶するクライアント情報部201と、ユーザID、パスワード、アクセスクラスなどを記憶するユーザ情報部202と、ベンダID、版数、グループ、レベルなどを記憶する認証クライアント識別情報部203と、アクセスクラス、ベンダID、版数、グループ、アクセス条件などを記憶するアクセス情報部204と、認証クライアントからの認証要求を受付ける処理受付部205と、処理受付部205で受付けた認証クライアントのIPアドレスや認証キーおよびユーザIDやそのパスワードなどが接続を許可してよいものかを確認する認証処理部206と、処理受付部205で受付けた認証クライアントに対応するアクセス条件をアクセス情報部204から取出すアクセス条件取出し部207と、認証結果およびアクセス条件を認証要求元に通知する結果通知部208とで構成されている。

【0016】また、認証サーバ2には、複数のベンダ固有のアクセス条件フォーマットを記憶するベンダ固有アクセス条件フォーマット部2011と、入力されたアクセス条件を記憶部などに格納するアクセス条件設定部2012と、ベンダ固有アクセス条件フォーマット部2011を参照し、アクセス条件設定部2012で格納されたアクセス条件をベンダ固有アクセス条件に変換するベンダ固有アクセス条件作成部2013とが備えられている。

【0017】図2に、本発明の一実施例の詳細な構成ブロック図を示す。図中、21は認証クライアント、22は認証サーバである。

【0018】認証クライアント21は、ユーザからのアクセスを受け、ユーザの認証要求を認証サーバ22に発行する処理依頼部211と、認証サーバ22からの認証結果を受取る結果受付部212と、認証結果で通知されたアクセス条件でユーザのアクセス許可／拒否を制御するアクセス制御部213とで構成されている。

【0019】認証サーバ22は、認証クライアントのIPアドレス、レベル、認証キーなどを記憶するクライアント情報部221と、ユーザID、パスワード、アクセスクラスなどを記憶するユーザ情報部222と、ベンダID、版数、グループ、レベルなどを記憶する認証クライアント識別情報部223と、アクセスクラス、ベンダID、版数、グループ、アクセス条件などを記憶するアクセス情報部224と、認証クライアントからの認証要求を受付ける処理受付部225と、処理受付部225で受付けた認証クライアントのIPアドレスや認証キーおよびユーザIDやそのパスワードなどが接続を許可してよいものかを確認する認証処理部226と、処理受付部225で受付けた認証クライアントに対応するアクセス条件をアクセス情報部224から取出すアクセス条件取出し部227と、認証結果およびアクセス条件を認証要求元の認証クライアント21に通知する結果通知部228とで構成されている。

【0020】また、認証サーバ22には、複数のベンダ固有のアクセス条件フォーマットを記憶するベンダ固有アクセス条件フォーマット部233と、入力されたアクセス条件を記憶部などに格納するアクセス条件設定部231と、ベンダ固有アクセス条件フォーマット部233を参照し、アクセス条件設定部231で格納されたアクセス条件をベンダ固有アクセス条件に変換するベンダ固有アクセス条件作成部232とが備えられている。

【0021】図3に、認証クライアント識別情報部、クライアント情報部、ユーザ情報部、アクセス情報部の構成例図を示す。図中、31は認証クライアント識別情報部、32はクライアント情報部、33はユーザ情報部、34はアクセス情報部である。

【0022】そして、認証クライアント識別情報部31は、認証クライアントのベンダを識別するベンダID、版数、グループと、認証クライアントを識別するためのレベルとで構成されている。

【0023】また、クライアント情報部32は、認証クライアントのIPアドレス、認証キーと、認証クライアントを識別するためのレベルで構成されている。

【0024】また、ユーザ情報部33は、ユーザIDと、そのパスワードとアクセスクラスとで構成されている。

【0025】また、アクセス情報部34は、アクセスクラスと、それに対応する認証クライアントのベンダID、版数、グループと、アクセス条件とで構成されている。

【0026】図4に、認証サーバの一実施例の処理フローチャートを示す。以下、図3の各情報部の構成例図と図4のフローに従って、動作を説明する。

【0027】ステップS401は、認証クライアントからの認証要求を処理受付部で受け、受け付けたデータからユーザID、そのパスワード、認証クライアントのIPアドレス、確認キーなどを獲得する。

【0028】ステップS402は、ステップS401で獲得した認証クライアントのIPアドレスに対応するレベルをクライアント情報部32から求め、そのレベルに対応するベンダID、版数、グループを認証クライアント識別情報部31から求める。なお、認証クライアントのIPアドレスや認証キーがクライアント情報部32で定義されていない、また、求めたレベルに対応するものが認証クライアント識別情報部31に定義されていない場合は異常となる。

【0029】ステップS403は、ステップS402が正常に完了したかを判定する。正常に完了したならば、ステップS404に進み、正常に完了していなければステップS408に進む。

【0030】ステップS404は、ステップS401で獲得したユーザID、パスワードに対応したアクセスクラスをユーザ情報部33から求める。なお、ユーザ情報部33にユーザIDが定義されていない、また、パスワードが誤っている場合は異常となる。

【0031】ステップS405は、ステップS404が正常に完了したかを判定する。正常に完了したならば、ステップS406に進み、正常に完了していなければステップS408に進む。

【0032】ステップS406は、ステップS402で求めた認証クライアント識別情報とステップS404で求めたアクセスクラスに対応するアクセス条件をアクセス情報部34から求める。

【0033】ステップS407は、アクセス許可情報と、ステップS406で求めたアクセス条件を認証クライアントに通知する。そして、処理を終了する。

【0034】ステップS408は、アクセス拒否情報を認証クライアントに通知する。そして、処理を終了する。

【0035】図5に、アクセス条件入力例とベンダ固有アクセス条件フォーマット部の構成例図を示す。図中、51はオペレータがアクセス条件設定部231において入力するアクセス条件入力例、52はベンダIDが‘00000001’のベンダ固有アクセス条件フォーマット部であり、その一部が示されている。

【0036】また、53はベンダ固有アクセス条件作成部232により作成されたベンダ固有アクセス条件部であり、アクセス条件入力例51からベンダ固有アクセス条件フォーマット部52のフォーマットをもとに作成されたものである。

【0037】図6に、ベンダ固有アクセス条件作成部の一実施例の処理フローチャートを示す。以下、このフローに従って、動作を説明する。

【0038】ステップS601は、アクセス条件設定部231において入力されたアクセス条件データを読み込む。

【0039】ステップS602は、ベンダ固有アクセス条件フォーマット部233に格納された全てのベンダ固有アクセス条件フォーマットについて作成したか判定する。作成したならば、処理を終了し、作成していなければステップS603に進む。

【0040】ステップS603は、複数のベンダ固有アクセス条件フォーマットが格納されたベンダ固有アクセス条件フォーマット部233から、ベンダのベンダ固有アクセス条件フォーマットを読み込む。

【0041】ステップS604は、ステップS601で読み込んだアクセス条件データの内容をステップS603で読み込んだベンダ固有アクセス条件フォーマットに従って定義し直し、ベンダ固有アクセス条件を作成する。そして、ステップS602に戻る。

【0042】

【発明の効果】この発明は、上記に説明したような形態で実施され、以下の効果がある。

【0043】ユーザ認証システムにおける認証サーバを、認証クライアントのIPアドレス、レベル、認証キーなどを記憶するクライアント情報部と、ユーザID、パスワード、アクセスクラスなどを記憶するユーザ情報部と、ベンダID、版数、グループ、レベルなどを記憶する認証クライアント識別情報部と、アクセスクラス、ベンダID、版数、グループ、アクセス条件などを記憶するアクセス情報部と、認証クライアントからの認証要求を受付ける処理受付部と、処理受付部で受付けた認証クライアントのIPアドレスや認証キーおよびユーザIDやそのパスワードなどが接続を許可してよいものかを確認する認証処理部と、処理受付部で受付けた認証クライアントに対応するアクセス条件をアクセス情報部から取出すアクセス条件取出し部と、認証結果およびアクセス条件を認証要求元に通知する結果通知部と、で構成することにより、複数の異なるベンダの認証クライアントから発行される認証要求を唯一つの認証サーバで受け取ることが可能となり、ユーザ認証を一元管理することが

できる。

【0044】また、上記の認証サーバに、複数のベンダ固有のアクセス条件フォーマットを記憶するベンダ固有アクセス条件フォーマット部と、入力されたアクセス条件を記憶部などに格納するアクセス条件設定部と、ベンダ固有アクセス条件フォーマット部を参照し、アクセス条件設定部で格納されたアクセス条件をベンダ固有アクセス条件に変換するベンダ固有アクセス条件作成部とを備えることにより、各ベンダの認証クライアントの仕様を熟知しなくても、容易に作成することが可能となり、認証クライアントの追加および変更などの認証システムの管理および運用を迅速に行うことができる。

【図面の簡単な説明】

【図1】 本発明のユーザ認証システムの構成ブロック例図である。

【図2】 本発明の一実施例の詳細な構成ブロック図である。

【図3】 認証クライアント識別情報部、クライアント情報部、ユーザ情報部、アクセス情報部の構成例図である。

【図4】 認証サーバの一実施例の処理フローチャートである。

【図5】 アクセス条件入力例とベンダ固有アクセス条件フォーマット部の構成例図である。

【図6】 ベンダ固有アクセス条件作成部の一実施例の処理フローチャートである。

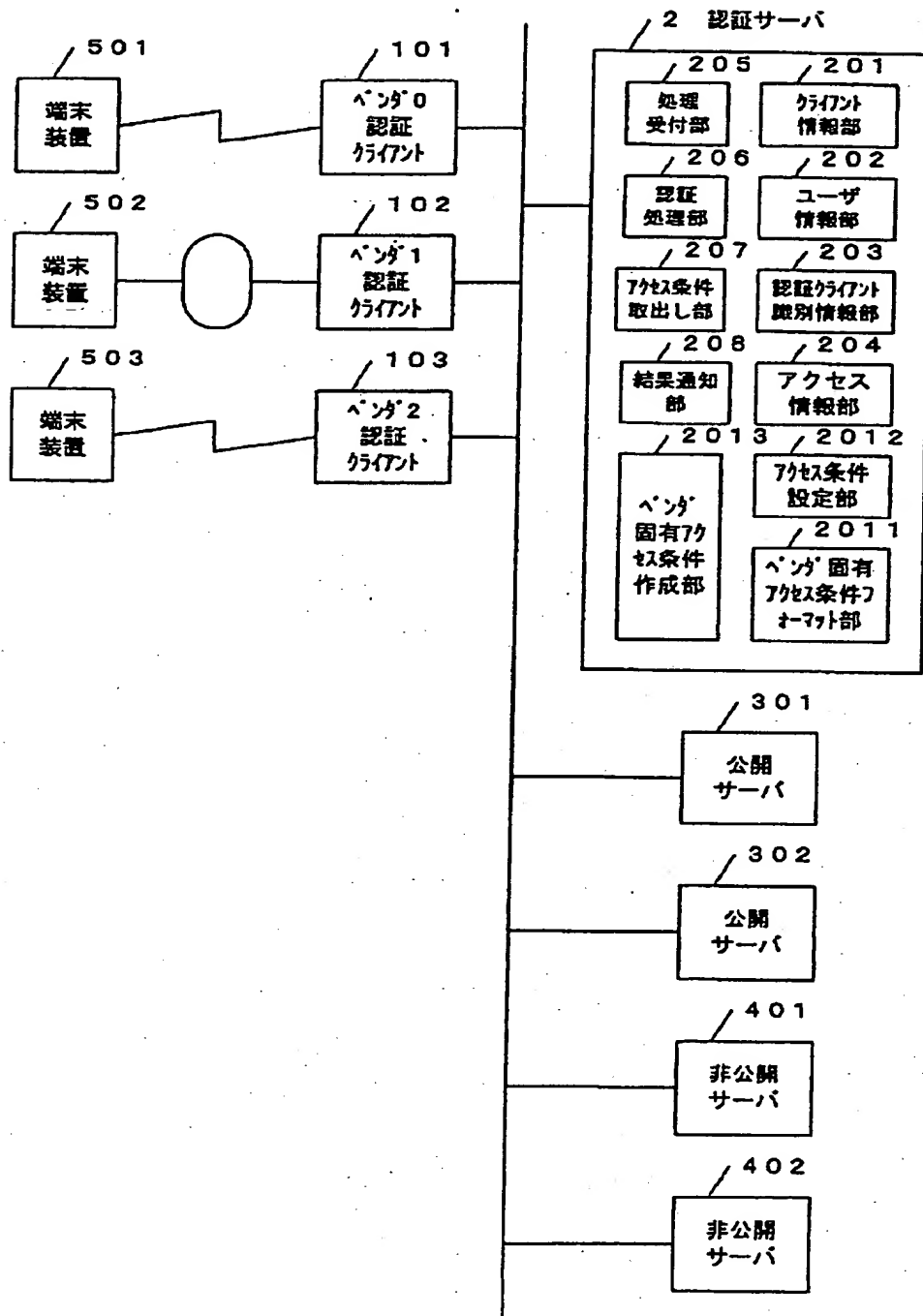
【図7】 従来のユーザ認証システムの構成ブロック例図である。

【符号の説明】

201	クライアント情報部
202	ユーザ情報部
203	認証クライアント識別情報部
204	アクセス情報部
205	処理受付部
206	認証処理部
207	アクセス条件取出し部
208	結果通知部
2011	ベンダ固有アクセス条件フォーマット部
2012	アクセス条件設定部
2013	ベンダ固有アクセス条件作成部

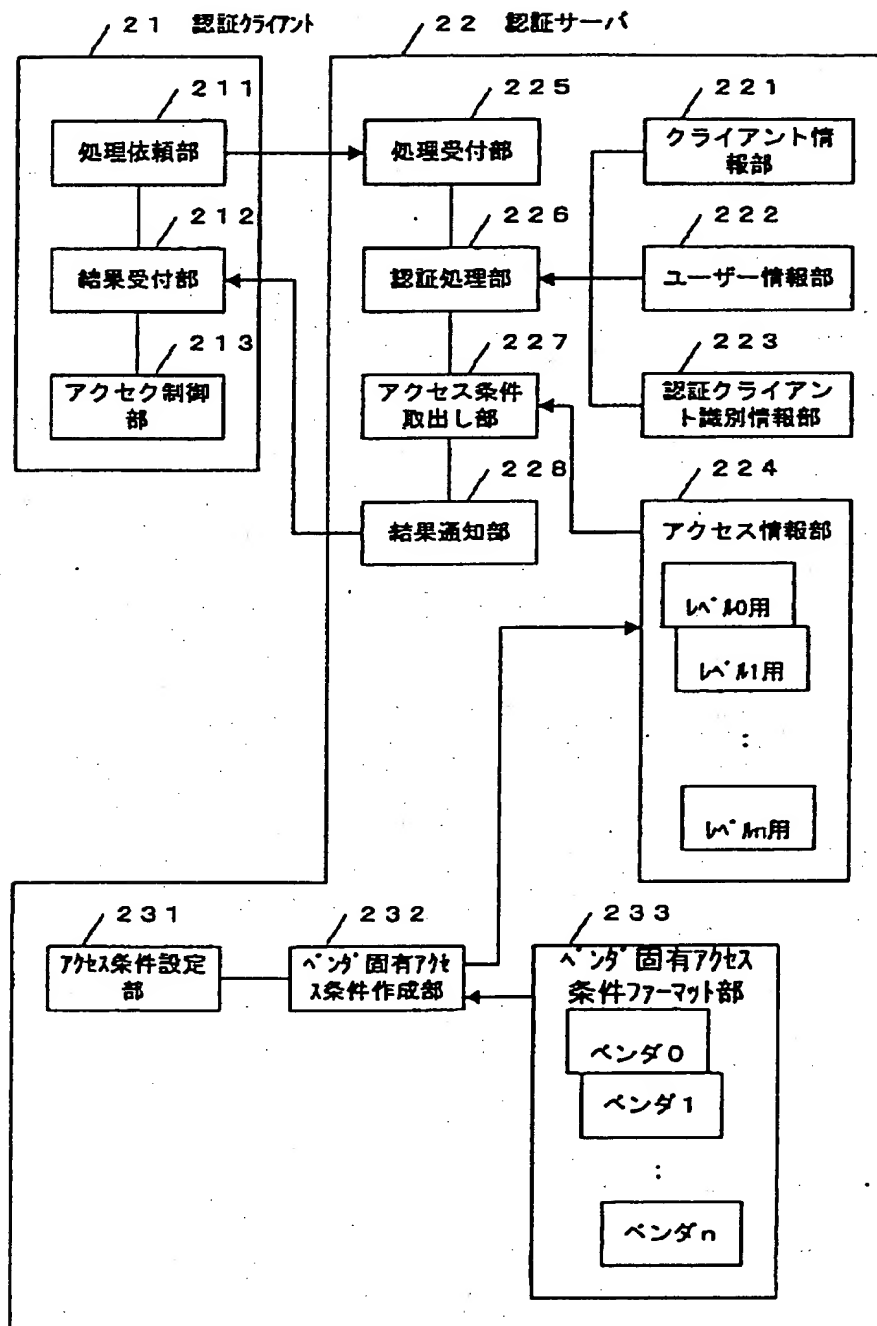
【図1】

本発明のユーザ認証システムの構成ブロック例図





### 本発明の一実施例の詳細な構成ブロック図



【図3】

認証クライアント識別情報部、クライアント情報部、ユーザ情報部、アクセス情報部の構成例図

## 31 認証クライアント識別情報部

ベンダID	版数	グループ	レベル
00000000	0001	0000	0000
00000001	0001	0000	0001
00000001	0002	0000	0002

## 32 クライアント情報部

IPアドレス	レベル	認証キー
192.0.0.1	0000	....
192.0.0.2	0000	....
192.0.0.3	0001	....
192.0.0.4	0001	....
192.0.0.5	0002	....

## 33 ユーザ情報部

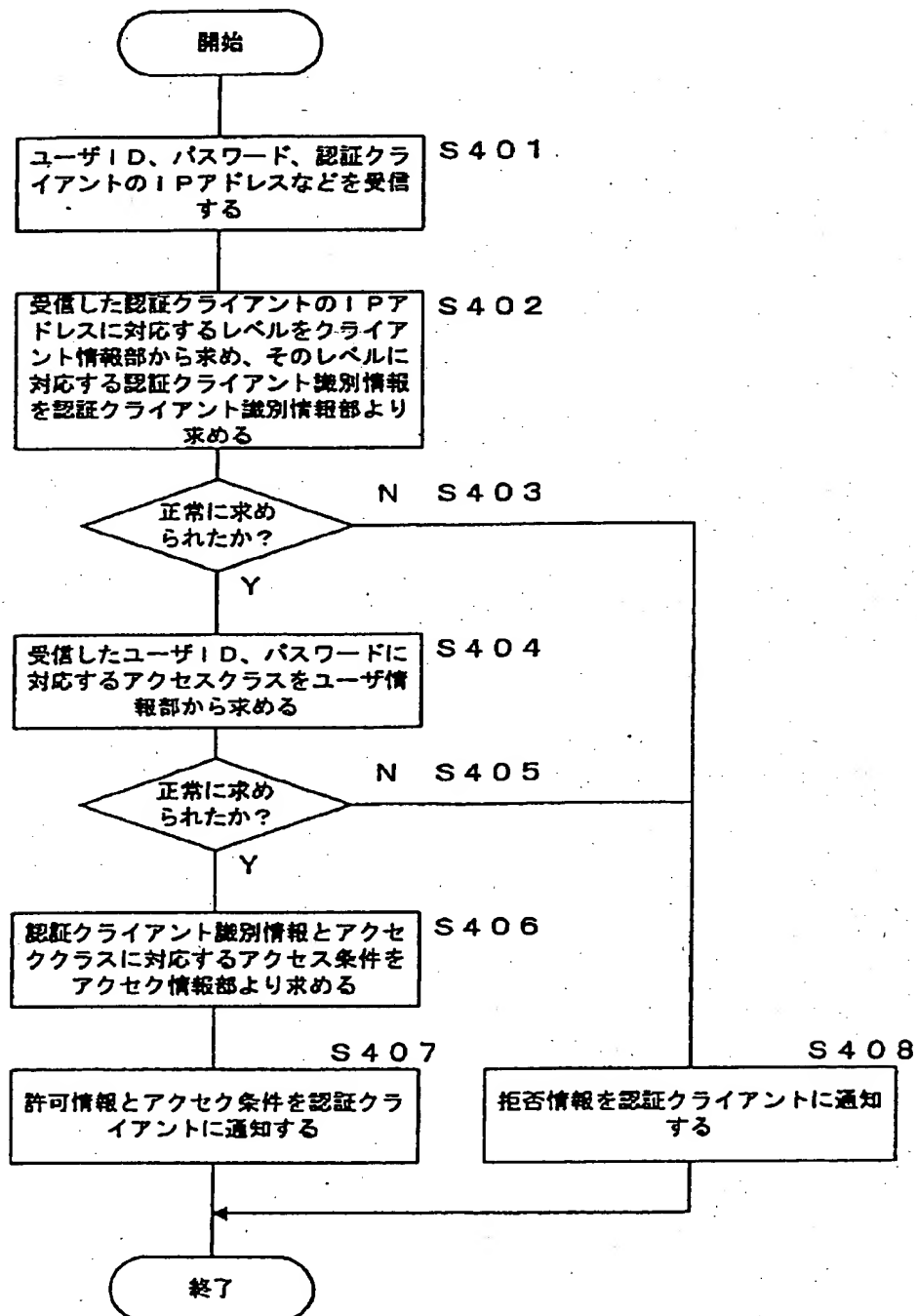
ユーザID	パスワード	アクセスクラス
macda	....	maneger
mimura	....	maneger
minamido	....	general
takagi	....	general
yoshida	....	general

## 34 アクセス情報部

アクセスクラス	ベンダID	版数	グループ	アクセク条件
maneger	00000000	0001	0000	レベル0用アクセス条件
maneger	00000001	0001	0000	レベル1用アクセス条件
general	00000001	0002	0000	レベル2用アクセス条件
general	00000000	0001	0000	レベル0用アクセス条件
general	00000001	0001	0000	レベル0用アクセス条件

【図4】

## 認証サーバの一実施例の処理フローチャート



【図5】

アクセス条件入力例とベンダ固有アクセス条件フォーマット部の構成例図

### 5.1 アクセス条件入力例

filter	
-s addr=192.0.0.0, mask=255.255.255.0	送信元のアドレスとマスク
-d addr=192.0.1.0, mask=255.255.255.0	送信先のアドレスとマスク
-f on	許可/拒否

### 5.2 ベンダ固有アクセス条件フォーマット部

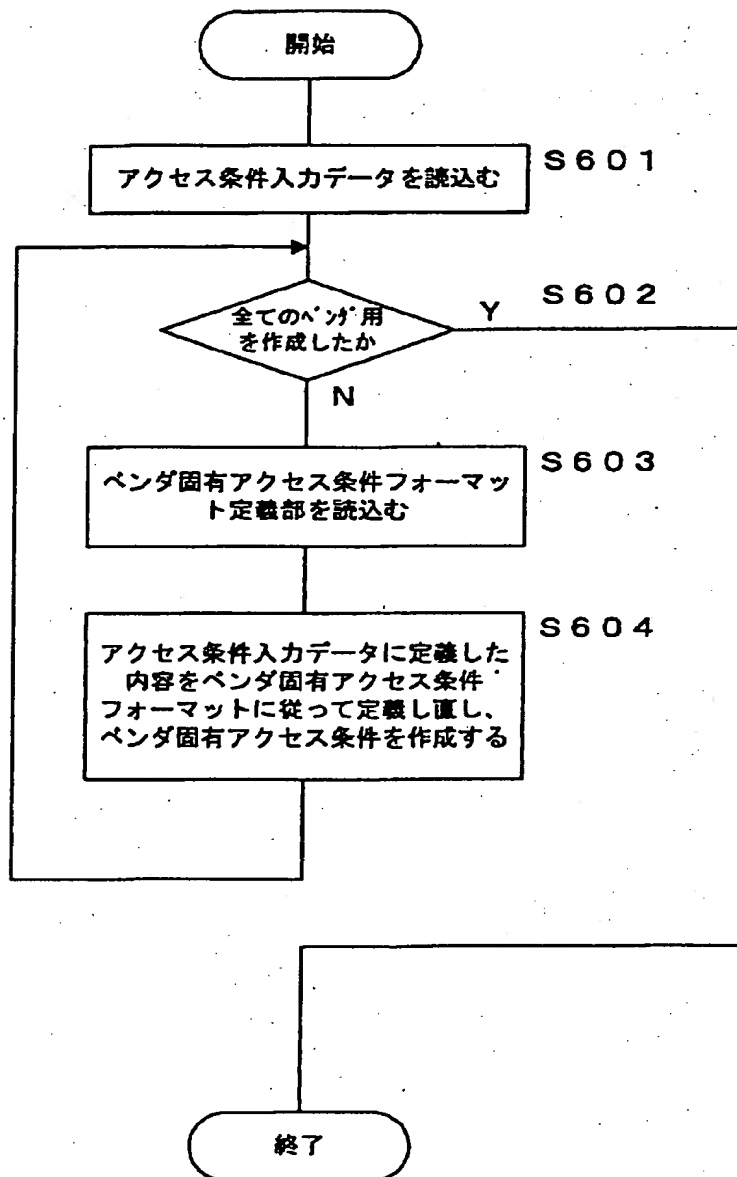
ベンダID	00000001
版数	0000
グループ	0000
属性番号=	200
src-addr	[送信元アドレス]
src-mask	[送信元マスク]
dest-addr	[送信先アドレス]
dest-mask	[送信先マスク]
flag	case on pass
	case off
	:
	:
	:
	:
	:

### 5.3 ベンダ固有アクセス条件部

属性番号=200
src-addr 192.0.0.0
src-mask 255.255.255.0
dest-addr 192.0.1.0
dest-mask 255.255.255.0
pass

【図6】

## ベンダ固有アクセス条件作成部の一実施例の処理フローチャート



【図7】

従来のユーザ認証システムの構成ブロック例図

